



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.813

(10/96)

SERIES X: DATA NETWORKS AND OPEN SYSTEM
COMMUNICATION

Security

**Information technology – Open Systems
Interconnection – Security frameworks in open
systems: Non-repudiation framework**

ITU-T Recommendation X.813

(Previously "CCITT Recommendation")

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS AND OPEN SYSTEM COMMUNICATION

PUBLIC DATA NETWORKS	X.1-X.199
Services and facilities	X.1-X.19
Interfaces	X.20-X.49
Transmission, signalling and switching	X.50-X.89
Network aspects	X.90-X.149
Maintenance	X.150-X.179
Administrative arrangements	X.180-X.199
OPEN SYSTEM INTERCONNECTION	X.200-X.299
Model and notation	X.200-X.209
Service definitions	X.210-X.219
Connection-mode protocol specifications	X.220-X.229
Connectionless-mode protocol specification	X.230-X.239
PICS proformas	X.240-X.259
Protocol Identification	X.260-X.269
Security Protocols	X.270-X.279
Layer Managed Objects	X.280-X.289
Conformance testing	X.290-X.299
INTERWORKING BETWEEN NETWORKS	X.300-X.399
General	X.300-X.349
Satellite data transmission systems	X.350-X.399
MESSAGE HANDLING SYSTEMS	X.400-X.499
DIRECTORY	X.500-X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600-X.699
Networking	X.600-X.629
Efficiency	X.630-X.649
Naming, Addressing and Registration	X.650-X.679
Abstract Syntax Notation One (ASN.1)	X.680-X.699
OSI MANAGEMENT	X.700-X.799
Systems Management framework and architecture	X.700-X.709
Management Communication Service and Protocol	X.710-X.719
Structure of Management Information	X.720-X.729
Management functions	X.730-X.799
SECURITY	X.800-X.849
OSI APPLICATIONS	X.850-X.899
Commitment, Concurrency and Recovery	X.850-X.859
Transaction processing	X.860-X.879
Remote operations	X.880-X.899
OPEN DISTRIBUTED PROCESSING	X.900-X.999

For further details, please refer to ITU-T List of Recommendations.

FOREWORD

ITU (International Telecommunication Union) is the United Nations Specialized Agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the ITU. Some 179 member countries, 84 telecom operating entities, 145 scientific and industrial organizations and 38 international organizations participate in ITU-T which is the body which sets world telecommunications standards (Recommendations).

The approval of Recommendations by the Members of ITU-T is covered by the procedure laid down in WTSC Resolution No. 1 (Helsinki, 1993). In addition, the World Telecommunication Standardization Conference (WTSC), which meets every four years, approves Recommendations submitted to it and establishes the study programme for the following period.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC. The text of ITU-T Recommendation X.813 was approved on 5th of October 1996. The identical text is also published as ISO/IEC International Standard 10181-4.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

© ITU 1997

All rights reserved. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the ITU.

CONTENTS

		<i>Page</i>
1	Scope.....	1
2	Normative references	2
	2.1 Identical Recommendations International Standards	2
	2.2 Paired Recommendations International Standards equivalent in technical content	2
3	Definitions.....	2
	3.1 Basic Reference Model definitions	2
	3.2 Security Architecture definitions	2
	3.3 Security Frameworks Overview definitions.....	3
	3.4 Additional definitions	3
4	Abbreviations	4
5	General discussion of Non-repudiation.....	4
	5.1 Basic concepts of Non-repudiation.....	4
	5.2 Roles of a Trusted Third Party.....	5
	5.3 Phases of Non-repudiation.....	5
	5.4 Some forms of Non-repudiation services.....	7
	5.5 Examples of OSI Non-repudiation evidence	8
6	Non-repudiation policies	8
7	Information and facilities	9
	7.1 Information	9
	7.2 Non-repudiation facilities	10
8	Non-repudiation mechanisms.....	12
	8.1 Non-repudiation using a TTP security token (secure envelope).....	12
	8.2 Non-repudiation using security tokens and tamper-resistant modules.....	13
	8.3 Non-repudiation using a digital signature	13
	8.4 Non-repudiation using Time Stamping.....	13
	8.5 Non-repudiation using an in-line Trusted Third Party.....	14
	8.6 Non-repudiation using a Notary.....	14
	8.7 Threats to Non-repudiation	14
9	Interactions with other security services and mechanisms.....	16
	9.1 Authentication.....	16
	9.2 Access Control.....	16
	9.3 Confidentiality	16
	9.4 Integrity.....	16
	9.5 Audit	16
	Annex A – Non-repudiation in OSI Basic Reference Model	17
	Annex B – Non-repudiation Facilities Outline	18
	Annex C – Non-repudiation in store and forward systems	19
	Annex D – Recovery in a Non-repudiation service.....	20
	Annex E – Interaction with the Directory	22
	Annex F – Bibliography	23

Summary

This Recommendation | International Standard defines a general framework for the provision of non-repudiation services. The goal of the Non-repudiation service is to collect, maintain, make available, and validate irrefutable evidence regarding identification of originators and recipients involved in data transfers.

Introduction

The goal of the Non-repudiation service is to collect, maintain, make available and validate irrefutable evidence concerning a claimed event or action in order to resolve disputes about the occurrence or non-occurrence of the event or action. The Non-repudiation service can be applied in a number of different contexts and situations. The service can apply to the generation of data, the storage of data, or the transmission of data. Non-repudiation involves the generation of evidence that can be used to prove that some kind of event or action has taken place, so that this event or action cannot be repudiated later.

In an OSI environment (see CCITT Rec. X.800 and ISO 7498-2) the Non-repudiation service has two forms:

- Non-repudiation with proof of origin which is used to counter false denial by a sender that the data or its contents has been sent.
- Non-repudiation with proof of delivery which is used to counter false denial by a recipient that the data or its contents (i.e. the information that the data represents) has been received.

Applications which make use of OSI protocols may require other forms of the Non-repudiation service which are specific to particular classes of applications. For example, MHS (ITU-T Rec. X.402 | ISO 10021-2) defines the Non-repudiation of submission service, while the EDI Messaging System (see Recommendation X.435) defines the Non-repudiation of retrieval and Non-repudiation of transfer services.

The concepts in this framework are not limited to OSI communications but may be interpreted more broadly to include such uses as creation and storage of data for later use.

This Recommendation | International Standard defines a general framework for the provision of a Non-repudiation service.

This framework:

- expands upon the concepts of Non-repudiation services described in CCITT Rec. X.800 and ISO 7498-2 and describes how they may be applied to Open Systems;
- describes alternatives for the provision of these services; and
- explains the relationship of these services to other security services.

Non-repudiation services may require:

- adjudicators who will arbitrate disputes that may arise as a result of repudiated events or actions; and
- Trusted Third Parties who will assure the authenticity and integrity of the data to be used for the verification of evidence.

Page 11/100
p. iv

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

**INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION –
SECURITY FRAMEWORKS IN OPEN SYSTEMS:
NON-REPUDIATION FRAMEWORK****1 Scope**

This Recommendation | International Standard addresses the application of security services in an Open Systems environment, where the term “Open Systems” is taken to include areas such as Database, Distributed Applications, Open Distributed Processing and OSI. The Security Frameworks are concerned with defining the means of providing protection for systems and objects within systems, and with the interactions between systems. The Security Frameworks are not concerned with the methodology for constructing systems or mechanisms.

The Security Frameworks address both data elements and sequences of operations (but not protocol elements) which are used to obtain specific security services. These security services may apply to the communicating entities of systems as well as to data exchanged between systems, and to data managed by systems.

This Recommendation | International Standard:

- defines the basic concepts of Non-repudiation;
- defines general Non-repudiation services;
- identifies possible mechanisms to provide the Non-repudiation services;
- identifies general management requirements for Non-repudiation services and mechanisms.

As with other security services, Non-repudiation can only be provided within the context of a defined security policy for a particular application. The definitions of security policies are outside the scope of this Recommendation | International Standard.

The scope of this Recommendation | International Standard does not include specification of details of the protocol exchanges which need to be performed in order to achieve Non-repudiation.

This Recommendation | International Standard does not describe in detail the particular mechanisms that can be used to support the Non-repudiation services nor does it give details of the supporting security management services and protocols.

Some of the procedures described in this framework achieve security by the application of cryptographic techniques. This framework is not dependent on the use of a particular cryptographic or other algorithm or on particular cryptographic techniques (i.e. symmetric or asymmetric) although certain classes of Non-repudiation mechanisms may depend on particular algorithm properties. Indeed it is likely, in practice, that a number of different algorithms will be used. Two entities wishing to use cryptographically-protected data must support the same cryptographic algorithm.

[| NOTE – Although ISO does not standardize cryptographic algorithms, it does standardize the procedures used to register them in ISO/IEC 9979.]

A number of different types of standard can use this framework including:

- 1) standards that incorporate the concept of Non-repudiation;
- 2) standards that specify abstract services that include Non-repudiation;
- 3) standards that specify uses of a Non-repudiation service;
- 4) standards that specify the means of providing Non-repudiation within an open system architecture; and
- 5) standards that specify Non-repudiation mechanisms.

Such standards can use this framework as follows:

- standards of type 1), 2), 3), 4) or 5) can use the terminology of this framework;
- standards of type 2), 3), 4) or 5) can use the facilities defined in clause 7; and
- standards of type 5) can be based upon the classes of mechanism defined in clause 8.

2 Normative references

The following Recommendations and International Standards contain provisions, which through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

- ITU-T Recommendation X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*.
- ITU-T Recommendation X.509 (1993) | ISO/IEC 9594-8:1995, *Information technology – Open Systems Interconnection – The Directory: Authentication framework*.
- ITU-T Recommendation X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

2.2 Paired Recommendations | International Standards equivalent in technical content

- CCITT Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.

3 Definitions

3.1 Basic Reference Model definitions

This Recommendation | International Standard builds on concepts developed in ITU-T Rec. X.200 | ISO/IEC 7498-1 and makes use of the following term defined in it:

(N)-entity.

3.2 Security Architecture definitions

This Recommendation | International Standard builds on the concepts developed in CCITT Rec. X.800 and ISO 7498-2 and makes use of the following terms defined in it:

- access control;
- audit (also security audit);
- authentication;
- channel;
- cryptographic checkvalue;
- cryptography;
- data integrity (also integrity);
- data origin authentication;
- decipherment;

- digital signature (also signature);
- encipherment;
- key;
- key management;
- notarization;
- repudiation;
- security audit trail (also audit trail, log);
- threat.

3.3 Security Frameworks Overview definitions

This Recommendation | International Standard builds on the concepts developed in ITU-T Rec. X.810 | ISO/IEC 10181-1 and makes use of the following terms defined in it:

- certification authority;
- digital fingerprint;
- hash function;
- one-way function;
- private key;
- public key;
- revocation list certificate;
- seal;
- sealed;
- secret key;
- security certificate;
- security domain;
- security token;
- trusted third party.

3.4 Additional definitions

For the purposes of this Recommendation | International Standard, the following definitions apply:

3.4.1 compromised evidence: Evidence that was, at one time, satisfactory but which no longer has the confidence of the Trusted Third Party or adjudicator.

3.4.2 counter-signature: A digital signature appended to a data unit which has already been signed by a different entity (e.g. a TTP).

3.4.3 evidence: Information that, either by itself or when used in conjunction with other information, may be used to resolve a dispute.

3.4.4 evidence generator: An entity that produces Non-repudiation evidence.

NOTE – This entity may be the Non-repudiation service requester, the originator, the recipient or multiple parties working in conjunction (e.g. a signer and co-signer).

3.4.5 evidence subject: The entity whose involvement in an event or action is established by evidence.

3.4.6 evidence user: An entity that uses Non-repudiation evidence.

3.4.7 evidence verifier: An entity that verifies Non-repudiation evidence.

3.4.8 message authentication code: A cryptographic checkvalue that is used to provide data origin authentication and data integrity.

3.4.9 Non-repudiation service requester: An entity that requests that Non-repudiation evidence be generated for a particular event or action.

3.4.10 notary: A Trusted Third Party with whom data is registered so that later assurance of the accuracy of the characteristics of the data can be provided.

3.4.11 originator: In the context of data transfer, an entity that originates the data in an action that is subject to a Non-repudiation service.

3.4.12 recipient: In the context of data transfer, an entity that receives the data in an action that is subject to a Non-repudiation service.

NOTE – In the logical model of Non-repudiation, other entities may be considered. E.g. the owner is the entity that makes an original message and a transfer agent is the entity that transfers the message; in this context, entities are modeled as originators or recipients.

4 Abbreviations

OSI	Open Systems Interconnection
CA	Certification Authority
TTP	Trusted Third Party
MAC	Message Authentication Code

5 General discussion of Non-repudiation

5.1 Basic concepts of Non-repudiation

The Non-repudiation service involves the generation, verification and recording of evidence, and the subsequent retrieval and re-verification of this evidence in order to resolve disputes. Disputes cannot be resolved unless the evidence has been previously recorded.

The purpose of the Non-repudiation service described in this framework is to provide evidence about a particular event or action. Non-repudiation services may be requested by entities other than those involved in the event or action. Examples of actions which may be protected with a Non-repudiation service are:

- sending an X.400 message;
- inserting a record in a database; and
- invoking a remote operation.

When messages are involved, to provide proof of origin, the identity of the originator and the integrity of the data must be confirmed. To provide proof of delivery, the identity of the recipient, and the integrity of the data must be confirmed. In some cases, evidence concerning the context (e.g. date, time, location of the originator/recipient) may also be required.

The service provides the following facilities which can be used in the event of an attempted repudiation:

- generation of evidence;
- recording of evidence;
- verification of generated evidence;
- retrieval and re-verification of the evidence.

Disputes may be settled between parties directly through inspection of the evidence. However, a dispute may have to be resolved by an adjudicator who evaluates the evidence and determines whether or not the disputed action or event occurred. Adjudication can only be provided effectively if the parties to the dispute accept the authority of the adjudicator. For the evidence provided to be accepted by the adjudicator, it must usually be assured by one or more Trusted Third Parties. The adjudicator can optionally be the Trusted Third Party that assures the evidence. Non-repudiation mechanisms use a number of types of Trusted Third Parties and forms of evidence.